SBIR Phase I: Security and Privacy: Passwords for Real People

Award Information
Agency:
National Science Foundation

Branch:
N/A
Amount:
$150,000.00

Award Year:
2015
Program:
SBIR

Phase:
Phase I
Contract:
1519879

Agency Tracking Number:
1519879
Solicitation Year:
2015

Solicitation Topic Code:
IC
Solicitation Number:
N/A
Small Business Information
Neurocrypt
414 East First Street, Bloomington, IN, 47401
Hubzone Owned:
N

Socially and Economically Disadvantaged:
N
Woman Owned:
Y

Duns:
079489570

Principal Investigator
Name: Timothy Kelley
Phone: (812) 822-2497
Email: t34k3ttl3@gmail.com

Business Contact
Name: Timothy Kelley
Phone: (812) 822-2497
Email:&nbspt34k3ttl3@gmail.com

Research Institution
N/A

Abstract

The broader impact/commercial potential of this Small Business Innovation Research (SBIR) Phase I project is to enable individuals and businesses to create and manage the plethora of passwords required by today's information infrastructure. The National Cyber Leap Year initiative identified the need to change the game in cybersecurity, increasing costs for attackers and easing the burdens of self-defense. A broader impact of the proposal is changing the game in favor of defenders, against password guessing or masquerade attacks. The company's technology builds on the human strengths of linguistic diversity and contextual memory to solve the core challenges of passwords: lack of entropy, reuse, and lack of contextualization. People are asked to create passwords without thinking of the domain name, the purpose, the word "password", or the keyboard in front of them. Thus people cannot secure their accounts. The high potential of commercial payback is the protection of personal and commercial assets. Aligning human behaviors and incentives is a promising approach in designing technologies to address social engineering - a problem that has proven intractable in the face of current education, awareness, and technological efforts. This Small Business Innovation Research (SBIR) Phase I project offers a system that aligns human cognitive behavior with technological requirements for security by engaging episodic memory. Today when creating a password, people are presented with the requirements to create a random phrase, not to write it down, not to reuse it, not to forget it, and not use any available cues in this task. In short, it is not humanly possible to create and remember strong, complex passwords. The approach being developed in this project combines four innovative features. First, it is aligned with - instead of in opposition to - natural cognitive processes. Second, the very process of using photos to offer more randomness in passwords enables the creation of a visual cue that is linked to a specific password and site. Third, the technology's connection between that cue and the password makes identifying phishing easier for the targeted person, because uncued recall is more difficult than cued recall. Fourth, the creation of a domain-specific image that must be obtained from a domain-specific server to cue the recall requires phishing become a man in the middle attack. This increases attack difficulty and decreases difficulty of detection.

* information listed above is at the time of submission.